

## REMARKS

In the Office Action dated December 24, 2008, claims 20-26 were objected to because the Examiner stated each dependent claim currently beginning with "A method..." should begin with "The method..." and should use the term "further comprising" rather than "comprising". In response to this requirement that was made in the previous Office Action, Applicant stated that this is a purely stylistic preference on the part of the Examiner, and there is no statute or rule that imposes such a requirement. Applicant still does not agree that there is any basis to require such a change, but in order to advance prosecution, Applicant has amended the dependent claims as proposed by the Examiner. Applicant notes, however, that even the Heiden et al reference relied upon by the Examiner employs the style to which the Examiner has objected, as do United States Patent No. 6,044,350 cited in the Information Disclosure Statement filed on April 28, 2006, and United States Patent Application Publication No. 2002/0108042 and United States Patent No. 5,742,684 cited in the Information Disclosure Statement filed April 18, 2005. Therefore, the Examiner's preference is clearly not shared by others in the Patent and Trademark Office, and these other patents are clearly evidence, as noted by the Applicant, that there is no statutory requirement to substantiate the Examiner's preference.

The claims also were objected to because the Examiner stated significant limitations should each begin with an indentation, and the claims have been editorially amended to comply with this requirement.

Claims 1 and 20-26 also were rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. Editorial changes have been made in the claims consistent with the recently-articulated requirements of the United States

Court of Appeals for the Federal Circuit in the *in re Bilski*, decision. All claims of the application are therefore submitted to be directed to statutory subject matter in accordance with the requirements of 35 U.S.C. §101.

Claims 1 and 20-26 were rejected under Section 112, first paragraph as failing to comply with the written description requirement, because the Examiner stated the step of “entering an input set..” is not supported in the present specification, including the portion referring to “an entry designating whether said communication is for said first purpose or said second purpose.”

This rejection is respectfully traversed, because each of Figures 2 and 5a through 9 clearly show the input (entry) of a communication m and an input c from the host device that operates the switch 24. The first paragraph at page 7 of the present specification makes clear that when the communication M is supplied to the input of the crypto logic module 20, it is accompanied by an input that operates (switches) the switch device 24 in order to designate whether crypto algorithm 1 or crypto algorithm 2 should be employed.

Claims 1 and 20-26 are therefore submitted to be fully supported in the present specification in accordance with the provisions of Section 112, first paragraph.

Claims 1 and 20-26 also were rejected under Section 112, second paragraph for the reasons noted by the Examiner at page 5 of the Office Action. The claims have been amended to respond to each of the bases for this rejection, and are submitted to be in full compliance with all provisions of Section 112, second paragraph. Claims 1, 20, 25 and 26 were rejected under 35 U.S.C. §103(a) as being

unpatentable over Heiden et al in view of a reference designated “Keytool”. This rejection is respectfully traversed for the following reasons.

As noted in Applicant’s previous response, the Examiner has acknowledged that the Heiden et al reference does not disclose that the cryptographic algorithms of the first and second types, when operating on the same input set, respectively generate different outputs. For this claim language, the Examiner relied on the Keytool reference as, according to the Examiner, teaching cryptographic algorithms of a first type and a second type that, for the same input set, respectively generate different outputs. The Examiner cited the RSA and DSA signatures described at page 4 of the Keytool reference for this purpose.

As also previously argued by the Applicant, the Keytool reference merely describes a library or storage location for different types of signatures. Two examples of these different types of stored signatures, as noted by the Examiner, are an RSA signature and a DSA signature. As explicitly stated at page 4 of the Keytool reference, however, the particular algorithm that is used is strictly dependent on the type of key that is intended to be used. Therefore, different keys result in the use of different algorithms, and thus result in the output of different signatures.

As noted by the Examiner, the Heiden et al reference discloses the use of different cryptographic algorithms respectively for different types of communications. Those different algorithms in Heiden et al, however, operate on *different* inputs, corresponding to the different types of communications that are intended. By contrast, in the subject matter of claim 1, the same input is supplied to the processor regardless of which type of communication is intended, and this current communication is input accompanied by a designation as to which communication

purpose is intended for that communication. Dependent on the communication purpose, the appropriate one of the two available cryptographic algorithms is selected, and this also results in a designation that one of the two signature possibilities will then be employed. The algorithms, and thus on the signatures, act on the same input.

Therefore, even if the Heiden et al reference were provided with a library of the type disclosed in the Keytool reference, this would not result in any significant difference in the operation of the Heiden et al system. The different signatures available in the Keytool library would simply be accessed for the different types of communications disclosed in the Heiden et al reference. In the Heiden et al reference, however, it is the input set for a particular communication, which will be the current communication, that determines or causes a particular algorithm to be employed. If it were desired in the Heiden reference to use the *same* input set for either type of communication, with the only difference then being which type of signature were employed dependent on which type of communication purpose is intended, it is not even clear that the Heiden et al system could function. In the Heiden et al system, it is essential that two *different* input sets be used for the respective different types of communication purposes. It is because these two *different* input sets are used in the Heiden et al reference, that the processor therein then "knows" which type of encryption algorithm should be employed.

For the reasons, Applicant submits that none of claims 1, 20, 25 or 26 would have been obvious to a person of ordinary skill in the field of cryptographically securing communications, under the provisions of 35 U.S.C. §103(a), based on the teachings of Heiden et al and the Keytool reference.

Claims 21-24 were rejected under 35 U.S.C. §103(a) based on the combination of Heiden et al and the Keytool reference, and further based on Official Notice of certain facts taken by the Examiner. Even if the Official Notice taken by the Examiner is correct, Applicant submits that the above arguments traversing the Examiner's conclusions regarding the Heiden et al/Keytool combination are applicable as well to the rejection of these dependent claims. For the same reasons, none of claims 21-24 would have been obvious to a person of ordinary skill in the field of cryptographically securing communications, under the provisions of 35 U.S.C. §103(a), based on the teachings of Heiden et al and the Keytool reference and the Official Notice taken by the Examiner.

All claims of the application are therefore submitted to be in condition for allowance, and early reconsideration of the application is respectfully requested.

The Commissioner is hereby authorized to charge any additional fees which may be required, or to credit any overpayment to account No. 501519.

Submitted by,



(Reg. 28,982)

---

SCHIFF, HARDIN LLP  
**CUSTOMER NO. 26574**  
Patent Department  
6600 Sears Tower  
233 South Wacker Drive  
Chicago, Illinois 60606  
Telephone: 312/258-5790  
Attorneys for Applicant.

CH1\6297220.1